PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-123950

(43)Date of publication of application : 15.05.1998

---

(51)Int.Cl. G09C 1/00

---

(21)Application number : 08-278423 (71)Applicant : FUJI XEROX CO LTD

(22)Date of filing : 21.10.1996 (72)Inventor : SAITO KAZUO
SHIN YOSHIHIRO
TAKEDA YUKIFUMI

---

(54) DATA VERIFICATION METHOD, VERIFIED DATA GENERATION DEVICE, AND DATA VERIFICATION DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To make it possible to use a protection device with a low calculation ability and a small storage capacity when securing to safely transmit or keep data like a history of utilization by adding verification value to them.

SOLUTION: A token 12 generates information on the utilization history and sends it to an information processing device 11, and also generates a verification value for holding it to a verification value holding part 21. The information processing device 11 records the information on the utilization history in a history holding part 16. The token 12 provides the verification value with a signature when requested for a verification output from the information processing device. The information processing device 11 outputs the information on utilization history and the verification value with the signature to a

recovery device 13. The recovery device 13 verifies the signature, and further, verifies the history of utilization based on the verification value.

LEGAL STATUS [Date of request for examination] 18.09.1998
[Date of sending the examiner's decision of rejection] 30.05.2003
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number] 3570114
[Date of registration] 02.07.2004
[Number of appeal against examiner's decision of rejection] 2003-012149
[Date of requesting appeal against examiner's decision of rejection] 30.06.2003
[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] In the interior of the equipment defended from the verification value of the body of data concerned, and the body of data preceded with the body of data concerned in the verification value of the body of data concerned about each of two or more bodies of data generated one by one The step which gives a digital signature to the verification value generated to the step to generate and the body of data of the last of two or more bodies of data verified at once in the interior of the equipment by which defense was carried out [above-mentioned], and generates a verification value with a signature, The data verification approach characterized by having the step which verifies two or more above-mentioned bodies of data based on the step which sends out the above-mentioned verification value with a signature to the exterior of the equipment by which defense was carried out [above-mentioned], two or more above-mentioned bodies of data, and the above-mentioned verification value with a signature.

[Claim 2] A means to generate the body of data one by one, and a verification value maintenance means to hold a verification value, a verification value new from the verification value currently held in the above-mentioned verification value maintenance means, and the newly generated body of data -- generating -- the above -- with a verification value generation means to update the verification value currently held with a new verification value at the above-mentioned verification value maintenance means Identity data-ed generation equipment characterized by having a signature means to sign the verification value currently held in predetermined timing at the above-mentioned verification value maintenance means, and establishing the above-mentioned verification value generation means, a verification value maintenance means, and the above-mentioned signature means in the defended equipment further.

[Claim 3] The data-verification equipment two or more above-mentioned bodies of data received carry out having a verification means verify the right thing as the description from the verification value with which a signature was verified by means receive the verification value with a signature with which a signature was performed to the verification value calculated from two or more bodies of data generated one by one, and two or more above-mentioned bodies of data, signature verification means verify the signature of the above-mentioned verification value with a signature which received, and the above-mentioned signature verification means.

[Claim 4] The hysteresis maintenance approach characterized by giving a digital signature only to the above-mentioned verification value in case only the only

verification value by which sequential count is carried out is held in the defended equipment to the historical-data group which consists of historical data which plurality followed and the above-mentioned verification value is outputted to the exterior of the equipment by which defense was carried out [above-mentioned].
[Claim 5] The data input means for inputting the data with which plurality continued, and the data-processing means for processing the above-mentioned data, The historical data relevant to processing of the above-mentioned data and the verification value held at the time are considered as an input. The verification value generation means for generating a verification value, and the verification value maintenance means for holding the generated above-mentioned verification value, The hysteresis supporting structure characterized by having a signature means for signing to this verification value, and holding the above-mentioned verification value generation means, the above-mentioned verification value maintenance means, and the above-mentioned signature means in the defended equipment at least.
[Claim 6] The hysteresis supporting structure according to claim 5 whose count used for the above-mentioned verification value generation means is a tropism function on the other hand.
[Claim 7] The hysteresis supporting structure according to claim 5 or 6 whose format of the above-mentioned historical data is a group with the verification value when processing a historical-data body and its historical data.
[Claim 8] The hysteresis supporting structure according to claim 5, 6, or 7 which it has a counter means to count whenever it processes data, and the format of the historical data in the above-mentioned historical-data group becomes from the value and hysteresis body of a counter when processing data.
[Claim 9] The hysteresis supporting structure according to claim 5, 6, 7, or 8 which outputs the signed verification value according to a user's output request.
[Claim 10] The hysteresis supporting structure according to claim 5, 6, 7, 8, or 9 to which the above-mentioned hysteresis supporting structure consists of single CPUs and software, and the above-mentioned signature means creates and outputs the verification value which signed the verification value suitably when the load of CPU by the data-processing means is low.
[Claim 11] It is the hysteresis supporting structure according to claim 5, 6, 7, 8, 9, or 10 in which the function of the above-mentioned data-processing means is suspended when the above-mentioned verification value is outputted, a data-processing means and, a just instruction is given to from the outside, and until has further a stall means to suspend the function of a ** data-processing means.

[Claim 12] The hysteresis supporting structure of a publication according to claim 11 which it has a condition precedent maintenance means for stopping a function, the above-mentioned stall means outputs the verification value with a signature which signed the above-mentioned verification value when the conditions described by the condition precedent maintenance means are fulfilled, and suspends a function.
[Claim 13] It has a just public key maintenance means for holding an external just person's public key. An external just person performs electronic signature to the verification value which the instruction which the above-mentioned stall means receives in order to return a function outputted at the end. The hysteresis supporting structure according to claim 11 or 12 which checks whether the verification value which a signature is verified and is further signed with the public key currently held at this just public key maintenance means when the above-mentioned stall means receives an instruction is equal to the verification value currently held at the above-mentioned verification value maintenance means.
[Claim 14] The data input means for inputting the verification value with a signature with which the signature was performed to the verification value calculated from two or more continuous historical-data groups and those data constellations, Hysteresis verification equipment characterized by having a verification means for the inputted above-mentioned data constellation verifying the right thing from the signature verification means for verifying the signature of the inputted above-mentioned verification value with a signature, and the inputted above-mentioned data constellation and the verification value with which the signature was verified.
[Claim 15] Hysteresis verification equipment according to claim 14 which also uses this pre-verification value in case it has a pre-verification value storage means for memorizing the verification value inputted into last time and a verification means verifies.
[Claim 16] Hysteresis verification equipment according to claim 14 or 15 whose count used for the above-mentioned verification means is a tropism function on the other hand.
[Claim 17] Hysteresis verification equipment according to claim 14, 15, or 16 whose format of the above-mentioned historical data is a group with the verification value when processing a historical-data body and its historical data.
[Claim 18] Hysteresis verification equipment according to claim 14, 15, 16, or 17 with which the format of the historical data in the above-mentioned historical-data group consists of the value and hysteresis body of a counter when processing data.
[Claim 19] The data storage means for holding data, and the condition precedent

maintenance means for holding the certain conditions which are at the time of suspending a function, The stall means for continuing suspending a function until it suspends a function and a just instruction is given from the outside, when the conditions held at this condition precedent maintenance means are fulfilled, The private key maintenance means for holding a private key, and the electronic office expert stage for performing electronic signature to the data constellation held at the data-hold means using the private key held at this private key maintenance means, It has an electronic signature maintenance means for holding the electronic signature which signed, and a just public key maintenance means for holding an external just person's public key. An external just person performs electronic signature to the electronic signature by which the instruction received in order that the above-mentioned stall means may return a function was held at the above-mentioned electronic signature maintenance means. The hysteresis supporting structure characterized by checking whether the value which a signature is verified and is further signed with the public key currently held at this just public key maintenance means when a stall means receives an instruction is equal to the value currently held at the electronic signature maintenance means.

[Claim 20] A stall means to suspend the function of some at least bodies of electronic equipment when predetermined conditions are fulfilled, A means to output predetermined data outside, and a means to receive the data with a signature generated by signing the above-mentioned predetermined data, Electronic equipment characterized by having a signature verification means to verify a signature about the above-mentioned data with a signature, and a means to cancel a halt of the function of the top Norikazu section when the justification of a signature of the above-mentioned data with a signature is verified by the above-mentioned signature verification means.

[Claim 21] A means to generate data one by one, and a verification value maintenance means to hold the verification value over the above-mentioned body of data, a verification value new from the verification value currently held in the above-mentioned verification value maintenance means, and the newly generated body of data -- generating -- the above -- with a verification value generation means to update the verification value currently held with a new verification value at the above-mentioned verification value maintenance means The data generation equipment which comes to have a signature means to sign the verification value currently held in predetermined timing at the above-mentioned verification value maintenance means, In the computer program product for performing interaction

between the data recovery systems which collect the bodies of data outputted from the above-mentioned data generation equipment The step which memorizes the verification value to which the body of data and signature which were outputted from the above-mentioned data generation equipment were performed, The computer program product characterized by using in order to make a computer perform the step which transmits the verification value to which the above-mentioned body of data and the above-mentioned signature which were memorized were performed to the above-mentioned data recovery system to predetermined timing.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Industrial Application] This invention relates about the technique of verifying data, to a lot of data constellations which continue especially, for example, the data verification technique suitable for using for the general information processor which must transmit or hold data like use hysteresis safely.

[0002]

[Description of the Prior Art] All information is digitized by development, an information highway design, etc. of a digital-information-processing technique for these days, and distribution and the circulating time are going to come through a network by them. As for text, various information, such as an image, an animation,

voice, and a program, is already beginning to distribute and circulate from the first with the gestalt of the Internet, personal computer communications, or CD-ROM.

[0003] however, a copy [a valueless copy is easy for it, and] of it at low cost if various digital information, such as such an alphabetic character, an image, an animation, voice, and a program, is not used since it does not have a stereo unlike a physical object -- etc. -- it has the description. However, since current has paid the countervalue to the possession, it has restricted that the information owned by a certain man is once copied. Originally, the lowness of the copy ease which must be the description which was most excellent in digital information, or its cost will be confined forcibly.

[0004] Encipher the digital information which makes a program representation recently in order to solve this, and it is made to circulate freely, in case it uses, price is paid, and a system which decrypts a receipt and information and uses the decode key for using digital information is also appearing. Or a technique which is charged from a viewpoint that it is valueless if information is not used, to informational use like the software service system in JP,6-95302,B and the amount measuring device of information use of JP,7-21276,A is proposed.

[0005] Accounting came to be made like [when purchase software when using the software to which a user makes a program representation on information processors, such as a personal computer and a workstation, with these techniques, and it does not use, but it receives no charge or very cheaply and it uses / since it is a form of a use tariff, for example, used once according to use] how much.

[0006] In order to charge to informational use, use tariffs must be collected from each user according to the frequency of the use. Or the use tariff which carried out package recovery depending on the case must be distributed to the side which offered information according to the use frequency. For that purpose, it is necessary to record the hysteresis of the use in a user's environment on insurance, and to collect safely.

[0007] However, although the amount meter of use exists in JP,7-21276,A as a function which records use hysteresis, it is not described how the amounts of use actually recorded there are collected.

[0008] There is the approach of recording use hysteresis on safe equipments which became independent of it, such as the store which the information processor which a user uses manages, for example, a hard disk drive unit etc., as an approach for that. For example, he is trying to write in the hysteresis of use in an IC card in JP,6-95302,B.

[0009] Moreover, he is trying to collect accounting information through a network in the accounting information collecting system of the accounting information sending-out method of JP,3-25605,A, or JP,6-180762,A.

[0010]

[Problem(s) to be Solved by the Invention] In order to collect the hysteresis written in safe equipment like an IC card, there is an approach which collects in a network or the recovery person who had just authority directly collects from the equipment directly.

[0011] However, by the method which collects hysteresis through a network, the safety of accounting information, i.e., accounting information, was not altered on the way, or the user created inaccurate accounting information and it was not taken into consideration at all about the field of the safety of being as sending it ****. Therefore, although it was applicable in the network which can set fixed reliance like [in a company], there was a problem that it was inapplicable from the field of safety in the Internet in which many and unspecified individuals participate.

[0012] Therefore, in order to collect the hysteresis in equipment like an IC card safely, the approach only had that the recovery person who had just authority directly collected from the equipment directly.

[0013] However, if the code technique in which recently comes and research is progressing, especially an electronic signature technique are used, it is possible to solve the above-mentioned problem. That is, to enclose the private key of a proper with a safety device, and in case data are picked out from a safety device, what is necessary is just surely made to sign. It can check now later by checking the electronic signature to which that data are right accompanies data by this.

[0014] The technique for which electronic signature uses a RSA (Rivest-Shamir-Adleman) code is known widely. However, general very much computational complexity is needed for the signature by RSA cryptograph, or other electronic signature, and, usually one processing takes great time amount. Therefore, when it must sign to a lot of continuous data, or in processing processing of a signature on a computer with low count capacity, it becomes a very big problem.

[0015] When equipment like an IC card as a safety device which records use hysteresis was used, generally, the count capacity of CPU which can be carried in such an IC card had many low things, and when a lot of count was carried out, the problem of taking time amount very much had it. Or in order to make computation time quick, when it was going to make count capacity high, the technical problem that very high cost was required occurred.

[0016] Moreover, since the historical data of use generally became huge, when it was

going to record all historical data on small equipment like an IC card, they also had the technical problem that storage capacity became a problem.

[0017] In addition, from the first, the safety of the code technique of the present age including RSA cryptograph has put the foundation on computational complexity, and if the capacity of a computer is extended, the key length used for a signature or a code in connection with it will be enlarged. Therefore, in using the devices (for example, token which an individual uses) which can use only the computer of a low throughput compared with a computer with the maximum throughput in not the problem of solving if the capacity of a computer will be improved in the future but that time, even if it crosses to the future, this problem always turns into an essential technical problem.

[0018] This invention is made in view of such a situation, and the place made into that purpose is to offer the approach of generating the data which can verify data at a high speed, even if it puts on the low equipment of count capacity.

[0019] That is, the whole use hysteresis does not tend to be held in an IC card, but you are going to hold only the verification value acquired from use hysteresis in an IC card, and are going to make it hold the body of use hysteresis to the information-processors (personal computer etc.) side which a user manages.

[0020] When a Prior art is referred to from a viewpoint of a verification value, there is a technique called DES-MAC which is the technique used for data communication. MAC is Message. Authentication It is the abbreviation for Code and a message is a code with the fixed die length which shows a perfect thing (not altered). It is used by being attached to an original message. Since it is fatal, that an error generates data communication on the way has composition which can detect that data have changed on the way.

[0021] Here, DES is Data. Encryption It is the algorithm of the block cipher which considers 64 bits as one block by the abbreviation for Standard (Applied Cryptography pp265). The CBC (CypherBlock Chain) mode (Applied Cryptography pp193, JIS-X5051) is a kind of the direction using the block cipher which makes DES representation, and it is the method which takes the exclusive OR of the block with which each block was made to become independent, and it did not encipher, but was enciphered [last], and the block which it is going to encipher from now on, and considers it as the input of DES. Even when it was this approach and the block of the same contents is enciphered, the results enciphered when the blocks enciphered by then differed will also differ.

[0022] DES-MAC (see the Applied Cryptography pp455 about CBC-MAC) tends to apply the CBC mode in DES, and tends to use for the verification value of the whole

data stream the block acquired at the end.

[0023] The configuration of DES-MAC is shown in drawing 21 . It is the data stream which the upper part of drawing tends to transmit, and a data stream is divided into the block of every 64 bits, respectively. It is Initial in IV. It is the initial value generated by the random numbers by the abbreviation for Vector. The divided block lets the DES code machine pass continuously like DES-CBC mode, adds the verification value of the data stream which is going to transmit IV and the block acquired by the last to a head, and is transmitted to it. In the side which received, it verifies whether the verification value acquired by performing processing contrary to this processing becomes equal.

[0024] However, fundamentally, if such an art aims at transmitting data by communication link and tends to apply to recovery of perfect hysteresis from a short time and holding certainly being the requisite about data with a perfect transmitting person, it will produce a problem. That is, it is because historical data may be accumulated over a long period of time and it may be put to risk, such as arbitrary management of a user and accident of a system, in the meantime.

[0025] It is premised on a data block being continuously transmitted in the first place by the above-mentioned approach (DES-MAC). That is, a low-ranking layer will usually exist in transmission of data further (TCP/IP: a TCP layer corresponds in a transmission control protocol / Internet Protocol), and the sequence of a data block will be guaranteed by the layer.

[0026] However, in the case of use hysteresis, if it puts under management of a user, the sequence of hysteresis will no longer be guaranteed at the time. That is, a user can be used, connecting an IC card to two or more computers with him (for example, Desktop PC, laptop PC, etc.). [usable] Considering that use hysteresis is recorded on a computer side, use hysteresis will be distributed by two or more computers. Therefore, the chronological sequence will be lost for the hysteresis distributed by two or more sets.

[0027] In the case of use hysteresis, time sequence serves as a very important element. That is, it is because the amount of use may be calculated later from the use hysteresis which plurality followed. For example, it is the case of calculating the utilization time from the difference of use start time and use end time in an easy example, or calculating the difference of the data length for actuation at the time of use initiation, and the data length for actuation to the data length at the time of use termination, and making it into the amount of use.

[0028] DES-MAC has not given essential solution to such technical problems.

[0029] Furthermore, I hear that those parts may be lost according to intentionally or accident, and one technical problem that I will accept it when use hysteresis is put under management of a user occurs. Verification will become impossible if the part is lost in DES-MAC. Since it is a premise that the transmitting person holds data only with between [perfect] communication links, in such a case, it can be managed with DES-MAC if it retransmits a message. However, in the case of use hysteresis, since hysteresis's being lost is that data are essentially lost, restoration is impossible. If the method of DES-MAC is used as it is, it will become impossible to perform even verification of the remaining data.

[0030] It is indispensable to collect the hysteresis left behind to the user further again in a system which performs the amount accounting of use. It is because there is a problem that a user's use tariff cannot be calculated or the collected use tariff cannot be distributed to an informational provider if hysteresis is not collected.

[0031] Therefore, the use hysteresis left behind to the user must be collected safely. As [be / recovery / by fake recovery instruction etc. / for that purpose, / made not to be performed]

[0032] Therefore, the place made into the purpose of this invention is to offer the equipment which can verify high-speed and huge data, even if count capacity is low and memory capacity is small.

[0033] Furthermore, the second purpose of this invention will offer the approach of restoring sequence also in an environment where the sequence of data is not saved.

[0034] Furthermore, the third purpose of this invention is offering the approach of verifying the remaining data, even when some data are lost.

[0035] Furthermore, the fourth purpose of this invention is to offer the approach of controlling the equipment holding data safely from the exterior.

[0036]

[Means for Solving the Problem] In order to reduce the amount of data fundamentally held in order to solve the above-mentioned technical problem, this invention does not record data in defense equipment, but outputs them out of defense equipment, and held the small verification value of the amount of data in defense equipment as that substitute. And with the concrete configuration, on the other hand, it was made to verify with a tropism function instead of electronic signature so that data could be verified at a high speed. When software realizes compared with encryption processing of RSA, the result that the hash value is quicker about triple figures has come out of the Hash Function which generally makes MD5 representation. Moreover, in order to enable restoration of the sequence of historical data especially, the information which

can restore sequence to historical data was added. Furthermore, in order to control defense equipment safely, specifically, it considered as the configuration which needs the value which gave the signature of a just person to the verification value which defense equipment holds. The verification value in defense equipment was compulsorily sent to the just person by this, and activation of verification is secured.

[0037] Furthermore, the configuration of this invention is explained. In order to attain the above-mentioned purpose according to this invention, it sets to the data verification approach. In the interior of the equipment defended from the verification value of the body of data concerned, and the body of data preceded with the body of data concerned in the verification value of the body of data concerned about each of two or more bodies of data generated one by one The step which gives a digital signature to the verification value generated to the step to generate and the body of data of the last of two or more bodies of data verified at once in the interior of the equipment by which defense was carried out [above-mentioned], and generates a verification value with a signature, It is made to perform the step which verifies two or more above-mentioned bodies of data based on the step which sends out the above-mentioned verification value with a signature to the exterior of the equipment by which defense was carried out [above-mentioned], two or more above-mentioned bodies of data, and the above-mentioned verification value with a signature.

[0038] In this configuration, count capacity may be [that what is necessary is just to give a digital signature to a verification value] low. Moreover, since verification comes out with the verification value over the body of data to precede, and this body of data and is calculated, if only one body of data and one verification value can be held, it can be processed, and its storage capacity may be small.

[0039] Moreover, a means to generate the body of data one by one in this invention to the identity data-ed generation equipment which generates the data for verification in order to attain the above-mentioned purpose, A new verification value is generated from the verification value currently held in a verification value maintenance means to hold a verification value, and the above-mentioned verification value maintenance means, and the newly generated body of data. the above -- with a verification value generation means to update the verification value currently held with a new verification value at the above-mentioned verification value maintenance means He establishes a signature means to sign the verification value currently held in predetermined timing at the above-mentioned verification value maintenance means, and is trying to establish the above-mentioned verification value generation means, the above-mentioned verification value maintenance means, and the

above-mentioned signature means in the defended equipment further.

[0040] Also in this configuration, count capacity may be [that what is necessary is just to give a digital signature to a verification value] low. Moreover, since verification comes out with the verification value over the body of data to precede, and this body of data and is calculated, if only one body of data and one verification value can be held, it can be processed, and its storage capacity may be small.

[0041] Moreover, two or more bodies of data generated one by one in order to attain the above-mentioned purpose according to this invention, A means to receive the verification value with a signature with which the signature was performed to the verification value calculated from two or more above-mentioned bodies of data, A verification means to verify that two or more received above-mentioned bodies of data are right from the verification value with which the signature was verified by signature verification means to verify the signature of the received above-mentioned verification value with a signature, and the above-mentioned signature verification means is made to prepare.

[0042] In this configuration, since what is necessary is just to perform verification of a signature to a verification value with a signature, computational complexity can be lessened.

[0043] Moreover, in order to attain the above-mentioned purpose according to this invention, in the hysteresis maintenance approach, in case the above-mentioned verification value is outputted to the exterior of the equipment by which defense was carried out [above-mentioned], it is made to hold only the only verification value by which sequential count is carried out in the defended equipment to the historical-data group which consists of historical data which plurality followed, and to give a digital signature only to the above-mentioned verification value.

[0044] Computational complexity and storage capacity can be stopped also in this configuration.

[0045] Moreover, the data input means for inputting the data with which plurality followed the hysteresis supporting structure, in order to attain the above-mentioned purpose according to this invention, The data-processing means for processing the above-mentioned data, and the historical data relevant to processing of the above-mentioned data, The verification value generation means for generating a verification value by considering the verification value held at the time as an input, He makes the verification value maintenance means for holding the generated above-mentioned verification value, and the signature means for signing to this verification value prepare, and is trying to hold in the equipment defended at least in

the above-mentioned verification value generation means, the above-mentioned verification value maintenance means, and the above-mentioned signature means.

[0046] Computational complexity and storage capacity can be stopped also in this configuration.

[0047] Moreover, on the other hand in this configuration, count used for the above-mentioned verification value generation means can be made into a tropism function. Moreover, the format of the above-mentioned historical data can be made into a group with the verification value when processing a historical-data body and its historical data. Moreover, a counter means to count whenever it processes data is established further, and the format of the historical data in the above-mentioned historical-data group can consist of the value and hysteresis body of a counter when processing data. Moreover, the signed verification value can be outputted according to a user's output request. Furthermore, the above-mentioned hysteresis supporting structure consists of single CPUs and software, and when the load of CPU by the data-processing means is low, the above-mentioned signature means creates the verification value which signed the verification value suitably, and can output.

[0048] Moreover, a data-processing means and when the above-mentioned verification value is outputted, the function of the above-mentioned data-processing means is suspended, and a just instruction is given from the outside and you may make it until establish further a stall means to suspend the function of a ** data-processing means, in this configuration. Moreover, the condition precedent maintenance means for stopping a function is established, and when the conditions described by the condition precedent maintenance means are fulfilled, the above-mentioned stall means outputs the verification value with a signature which signed the above-mentioned verification value, and you may make it suspend a function. Furthermore, it has a just public key maintenance means for holding an external just person's public key. An external just person performs electronic signature to the verification value which the instruction which the above-mentioned stall means receives in order to return a function outputted at the end. You may make it check whether the verification value which a signature is verified and is further signed with the public key currently held at this just public key maintenance means when the above-mentioned stall means receives an instruction is equal to the verification value currently held at the above-mentioned verification value maintenance means.

[0049] Moreover, the data input means for inputting into hysteresis verification equipment the verification value with a signature with which the signature was

performed to the verification value calculated from two or more continuous historical-data groups and those data constellations, in order to attain the above-mentioned purpose according to this invention, He is trying to establish a verification means for the inputted above-mentioned data constellation to verify the right thing from the signature verification means for verifying the signature of the inputted above-mentioned verification value with a signature, and the inputted above-mentioned data constellation and the verification value with which the signature was verified.

[0050] In this configuration, since it will end if a signature is verified to a verification value with a signature, computational complexity can be stopped.

[0051] Moreover, in case the pre-verification value storage means for memorizing the verification value inputted into last time is established and a verification means verifies, you may make it also use this pre-verification value in this configuration. Moreover, on the other hand, it is good also as a tropism function in the count used for the above-mentioned verification means. Moreover, the format of the above-mentioned historical data can be made into a group with the verification value when processing a historical-data body and its historical data. Furthermore, you may make it constitute the format of the historical data in the above-mentioned historical-data group from the value and hysteresis body of a counter when processing data.

[0052] Moreover, the data storage means for holding data to the hysteresis supporting structure, in order to attain the above-mentioned purpose according to this invention, The condition precedent maintenance means for holding the certain conditions which are at the time of suspending a function, The stall means for continuing suspending a function until it suspends a function and a just instruction is given from the outside, when the conditions held at this condition precedent maintenance means are fulfilled, The private key maintenance means for holding a private key, and the electronic office expert stage for performing electronic signature to the data constellation held at the data-hold means using the private key held at this private key maintenance means, The electronic signature maintenance means for holding the electronic signature which signed, and the just public key maintenance means for holding an external just person's public key are established. An external just person performs electronic signature to the electronic signature by which the instruction received in order that the above-mentioned stall means may return a function was held at the above-mentioned electronic signature maintenance means. He is trying to check whether the value which a signature is verified and is further signed with the public

key currently held at this just public key maintenance means when a stall means receives an instruction is equal to the value currently held at the electronic signature maintenance means.

[0053] In this configuration, the idle state of equipment is canceled only after the instruction with which the just person signed only after the justification of hysteresis was verified is sent and this just instruction is verified. Therefore, there is no un-arranging [that service continues being offered while just hysteresis has not been collected by it]. A paraphrase secures recovery of just hysteresis.

[0054] Moreover, a stall means according to this invention to suspend the function of some at least bodies of electronic equipment when predetermined conditions are fulfilled by electronic equipment, A means to output predetermined data outside, and a means to receive the data with a signature generated by signing the above-mentioned predetermined data, A signature verification means to verify a signature about the above-mentioned data with a signature, and a means to cancel a halt of the function of the top Norikazu section when the justification of a signature of the above-mentioned data with a signature is verified by the above-mentioned signature verification means are established.

[0055] In this configuration, use of electronic equipment can be continued only after the justification of data is checked. Therefore, just data are securable.

[0056] Moreover, this invention can realize that part as a computer program product.

[0057]

[The mode of implementation of invention]

The example of this invention is explained below the [1st example]. The 1st example is explained first. This example and other examples mentioned later are the systems that use the general digital information which are enciphered and are circulating, such as a program and image information, on information processors, such as a personal computer and a workstation, catch and record the timing which decodes information in the IC card (it is hereafter called a token) which connected the use hysteresis in that case to that information processor, and a pin center,large collects those use hysteresis. Of course, this invention is applicable besides security reservation of historical data.

[0058] Drawing 1 shows the overall configuration of this example. In drawing 1 , a personal computer, a workstation, etc. have the information processor 11 for using digital information in a user's environment, and in order to decode the enciphered information to it (or the key for decoding is decoded), the token 12 for catching the timing and recording use hysteresis is connected. The connection between a token 12

and an information processor 11 can use them anything, if a PC card (PCMCIA: personal computer memory card interface association) interface, a serial, parallel, infrared radiation, etc. are means by which information can be transmitted. It may be made to mount in the interior of an information processor 11.

[0059] A user's information processor 11 is connected if needed [the recovery system 13 and if needed] which consist of information processors by the side of a pin center,large, such as a workstation or a mainframe. The gestalt of connection is good at network interfaces, such as a modem, the telephone line, or Ethernet. It is enough, if this connection is not necessarily always made, and it is carried out from a user's information processor 11 only when use hysteresis needs to be collected.

[0060] The configuration of the information processor 11 by the side of a user is shown in drawing 2 . A user's information processor 11 is good by a common personal computer and a common workstation. Only the places where the token 12 is connected differ. An information processor 11 realizes a control section 14, the information attaching part 15, the hysteresis attaching part 16, and the hysteresis transmitting section 17. Such a configuration is realizable by installing the program concerned using record-medium 11a on which the program was recorded.

[0061] A control section 14 performs the following processings, communicating with a token 12.

** Perform or process the information which read the enciphered information which is stored in the information attaching part 15, and passes a token 12, and I had decode, and was decoded.

** When decode data are received, store in reception the use hysteresis passed to coincidence from a token 12, and store it in the hysteresis attaching part 16.

** In response to the directions from a user, give an instruction of a "verification value output" to a token 12, and pass the verification value to which the electronic signature which it is as a result was performed to the hysteresis transmitting section 17.

[0062] The data with which a user uses the information attaching part 15, and information or the enciphered data is stored. It consists of external storage, such as memory or a hard disk drive unit, in fact.

[0063] The hysteresis to which the hysteresis attaching part 16 was passed from the token 12 side through the control section 14 is stored. It consists of external storage, such as memory or a hard disk drive unit, in fact. About the concrete configuration of hysteresis, it mentions later.

[0064] The hysteresis transmitting section 17 reads the hysteresis currently held with

the verification value passed from the control section 14 at the hysteresis attaching part 16 in response to the instruction from a control section 14, and transmits to the recovery system 13 of a pin center,large. It consists of network interfaces, such as a modem, the telephone line, or Ethernet, etc. in fact. Or even if it is not a network, it once stores in equipments, such as a floppy disk, and a user may be made to input it into the recovery system 13 of a pin center,large with a help.

[0065] The configuration of the token 12 by the side of a user is shown in drawing 3 . A token 12 consists of general MPU, memory, etc. physically. It is stored in an attack confrontation container that itself reads the contents of memory or a token 12 breaks etc. so that it may be equal to a physical attack from the outside. Since an attack confrontation container is a well-known technique, explanation is omitted here (patent No. 186353, patent No. 1860463, JP,3-100753,A, etc.). In addition, whether what can be equal to attack [what] is chosen changes according to extent of the security of data. The offensive is weak.

[0066] It connects with a user's information processor 11, and a token 12 performs fixed processing according to the directions from an information processor 11, and returns the result. The token 12 has the user private key attaching part 18, the decode section 19, the verification value generation section 20, the verification value attaching part 21, the verification value output section 22, the token private key attaching part 23, and the electronic signature section 24 grade. Each configuration section of a token 12 is explained in full detail behind. A token 12 has the following functions.

[0067] ** Decode with the private key in which encryption data are stored in by reception from the maintenance (1) information processor 11 of an informational decode function and use hysteresis, and it is stored by the user private key attaching part 18, and return decode data to an information processor 11.

(2) Return to an information processor 11 by making the identifier into use hysteresis with reference to the information identifier currently described there with reference to the header of the data decoded while performing decode processing.

(3) Further, use hysteresis is also passed to the verification value generation section 20, and the verification value generation section 20 calculates to use hysteresis and the verification value currently held to the verification value attaching part 21 at the time, and stores the count result in the verification value attaching part 21.

[0068] ** Perform and return electronic signature to the verification value currently held to the verification value attaching part 21 at the time in response to the output request from the output functional information processor 11 of a verification value.

Then, the data in the verification value attaching part 21 are eliminated.

[0069] Hereafter, each configuration section of a token 12 is explained.

[0070] The decode section 19 performs decode processing using the private key of the user proper currently held in the passed encryption data at the user private key attaching part 18 responding to the decode demand from an information processor 11, and returns it to an information-processor 11 side by using the result as decode data. At this time, the header of the data decoded to it and coincidence is read, and while returning to an information-processor 11 side by making into use hysteresis the information identifier currently described there, the verification value generation section 20 is also passed (the information identifier of the used information is used for use hysteresis in this example).

[0071] Thus, with constituting, in case information is used, access to a token 12 is surely needed, and a user can record use hysteresis now certainly.

[0072] Here, what enciphered the key for decoding the information which the information itself could be enciphered and was enciphered is sufficient as the code data passed from an information-processor 11 side. Decode processing of an information body will be made by the information-processor 11 side at the case of the latter.

[0073] The user private key attaching part 18 holds the private key of a user proper. Generally, a token 12 is beforehand distributed to a user by the token issue pin center,large etc. in the form which enclosed the key of the proper for every user. Therefore, the user itself cannot know this user private key.

[0074] The verification value attaching part 21 holds only one verification value by which renewal of sequential is carried out. Generally a verification value is a value with the die length of immobilization, such as 16 etc. bytes. Therefore, if a verification value is 16 bytes, it consists of only 16 bytes of memory. The example of a configuration of a verification value is shown in drawing 4 .

[0075] The verification value output section 22 reads the verification value stored in the verification value attaching part 21 at the time in response to the output request of the verification value from an information-processor 11 side, and has the function to return it to an information-processor 11 side. In that case, the verification value output section 22 calls the electronic signature section 24, and performs electronic signature to a verification value.

[0076] The electronic signature section 24 performs processing which performs electronic signature to the given value using the private key held at the token private key attaching part 23 holding the private key only for the tokens. The token private

key attaching part 23 is the configuration section holding the private key for a signature used in case electronic signature is performed. It is possible to use electronic signature techniques, such as a RSA signature, for these configuration sections, and since it is a Prior art, detailed explanation is omitted here.

[0077] If use hysteresis (here information identifier) is received from the decode section 19, the verification value generation section 20 reads the verification value currently held at the verification value attaching part 21, and it will calculate a new verification value by performing the following count from use hysteresis and a verification value.

[0078]

[Equation 1] H=Hash(Usage+Hold)

Here, as for H, use hysteresis and Hash() mean a new verification value and a verification value current in Hold, on the other hand, Usage means a tropism function, and MD5, SHA (SecureHash Algorithm), etc. are used in fact. If its die length is the same, even if the operation "+" in this operation may actually do sums as a numeric value, and it will take an exclusive OR, it is also good to have arranged two data in order. make it any -- what is necessary is just to compound two values The verification value generation section 20 stores in the verification value attaching part 21 the new verification value calculated in this way (that is, an old value is overwritten).

[0079] The verification value output section 22 receives the output request from an information processor 11, and after it returns the verification value currently held to the verification value attaching part 21 at the time, it is made to initialize the verification value attaching part 21 to the value which was able to be decided beforehand. Or you may make it clear simply.

[0080] Next, the recovery system 13 of a pin center,large is explained. The configuration of a recovery system 13 is shown in drawing 5 . In drawing 5 , the recovery system 13 has the hysteresis receive section 25, the hysteresis attaching part 26, the hysteresis verification section 27, the token public key attaching part 28, and the signature verification section 29 grade. A recovery system 13 receives the hysteresis sent from a user's information processor 11 by the hysteresis receive section 25, and stores the contents in the hysteresis attaching part 26. The stored use hysteresis is read by the hysteresis verification section 27, it is verified whether it is the right and hysteresis is outputted to the manager by the side of a pin center,large by the result.

[0081] Generally, according to the contents of that hysteresis, a pin center,large

calculates an informational use tariff and performs after this processing in which the use tariff which collected that tariff from the user and collected it is distributed to an information provider according to the detail of informational use hysteresis. However, directly, since it is unrelated, explanation is abbreviated to the essence of this invention here.

[0082] Hereafter, each configuration section of a recovery system 13 is explained.

[0083] The hysteresis receive section 25 receives the hysteresis information sent from an information processor 11. It consists of information input units from the outside, such as network interfaces, such as a modem, the telephone line, or Ethernet, and a certain ** floppy disk drive unit, like the hysteresis transmitting section 17 (drawing 2) of an information processor 11 in fact. The use hysteresis received by the hysteresis receive section 25 is stored in the hysteresis attaching part 26.

[0084] Furthermore, in order to verify whether the verification value sent from the information processor 11 is just, it has the token public key attaching part 28 and the signature verification section 29.

[0085] If hysteresis is transmitted from an information processor 11, the hysteresis receive section 25 will receive. The received hysteresis is passed to the signature verification section 29 while it is stored in the hysteresis attaching part 26. The signature verification section 29 chooses the public key of a token 12 connected to the information processor 11 which has transmitted hysteresis from two or more token public keys stored in the token public key attaching part 28, and verifies the signature of hysteresis using the public key. The verification result is held with the hysteresis stored in the hysteresis attaching part 26. Since the verification value may have been altered or forged when the result that a verification result is a false came out, the following processings are not continued, but a message to that effect is outputted to a manager, and processing is suspended.

[0086] The following processings are continued when a signature is verified.

[0087] The hysteresis attaching part 26 holds the use hysteresis and the verification result which were passed from the hysteresis receive section 25. The hysteresis attaching part 26 consists of storage, such as memory, in fact.

[0088] The hysteresis verification section 27 is the following, and makes and verifies the hysteresis held at the hysteresis attaching part 26.

(1) It is the sequence of the transmitted hysteresis ud1, ud2, and ud3 ... It is referred to as udn.

(2) Set to hud the verification value attached to the last of hysteresis.

(3) If initial value of a verification value is set to ihud, according to the following

formulas, hud' which is the result of calculating will investigate whether it becomes equal to sent hud.

[0089]

[Equation 2] hud'=Hash(udn+Hash(udn-1+...Hash(ud2+Hash(ud1+ihud))...))

hud=?hud' (4) If equal, it will judge that it is not altered and that it is altered if not equal, and the manager of a recovery system will be notified of the result.

[0090] Next, the format of the information processed in each part is explained.

[0091] The format of the enciphered information which is set as the object of decode by the token 12 at drawing 6 is shown. (a) is the case where the information itself is enciphered with a user's private key. It is the case where it is said that (b) decodes what enciphered the private key used for enciphering an information body first with the private key of a user proper, and decodes an information body using the private key of the information proper obtained as a result. In (b), decode of an information body may be performed by the information-processor [not the token 12 but] side. Moreover, although the example which uses the common use code here is explained, it cannot be overemphasized that these may use a open code.

[0092] Here, an information identifier is an identifier of the information proper given when a pin center,large makes information encipher and makes it circulate. If an information identifier is managed by the pin center,large (it has a database) and an information identifier is specified, it can specify that the information is created by whom etc.

[0093] The format of use hysteresis is shown in drawing 7 . (a) is use hysteresis recorded in the information processor 11 in this example, and is the train of the used information identifier (information decoded by the token). (b) is use hysteresis sent to a pin center,large from an information processor 11, and only the places where the signature of the token to the verification value which a token holds at the last of (a), and a verification value is attached differ.

[0094] Although each use hysteresis is constituted from this example by only the used information identifier, as for this, the data of arbitration, for example, the used time of day, a user's identifier, the amount of use, the use amount of money, etc. may be contained. That is, since each hysteresis becomes long in leaving various information as hysteresis (it is generally common to leave various information as for hysteresis), this invention becomes effective.

[0095] Next, the processing in an information processor 11 and a token 12 is explained with reference to drawing 12 from drawing 8 . Drawing 8 is the flow of processing when there is a use demand of information from a user in the control section 14 of an

information processor 11. Drawing 9 is processing when there is similarly a use hysteresis recovery instruction from a user in a control section 14. Drawing 10 is processing when the decode section 19 of a token 12 receives a decode demand of the information enciphered from the information processor 11. Drawing 11 is processing of the verification value generation section 20 of the token 12 called from the decode section 19 of a token 12. Drawing 12 is processing when the verification value output section 22 of a token 12 receives a verification value output request from an information processor 11.

[0096] As shown in drawing 8 , when there is a demand of information use from a user, in the control section 14 of an information processor 11, processing progresses as follows. First, it distinguishes whether the information on target is enciphered (S11), and if not enciphered, information is processed as it is (S15). When enciphered, a decode demand is advanced to a token 12, and object information is handed over (S12). At this time, if an error is returned from a token 12, the error message "the hysteresis of a token is full" will be sent, and processing will be ended (S13, S16). If an error is not returned, the use hysteresis ****(ed) from the token 12 is recorded on recording devices, such as a disk, (S14). And object information is processed (S15).

[0097] As shown in drawing 9 , when there is a use hysteresis recovery instruction from a user, in the control section 14 of an information processor 11, processing progresses as follows. First, it distinguishes whether the information on target is enciphered (S21), and if not enciphered, information is processed as it is (S24). When enciphered, a decode demand is advanced to a token 12, and object information is handed over (S22). And the use hysteresis returned from the token 12 is recorded on recording devices, such as a disk, (S23). The information for after [this] is processed (S24).

[0098] As shown in drawing 10 , when the decode section 19 of a token 12 receives a decode demand of the information enciphered from the information processor 11, processing progresses as follows. First, the user private key Ku is taken out from the user private key attaching part 18 (S31). Encryption data are decoded with the user private key Ku, and decode data are memorized (S32). An information identifier is read with reference to the header of decode data, and call appearance necropsy certificate value generation processing is performed for the verification value generation section 20 by making this identifier into an argument (refer to S33, S34, and drawing 11). decode data and an identifier are returned to the information main cage right [that] value 35 after this (S35).

[0099] As shown in drawing 11 , when the verification value generation section 20 of a

token 12 is called from the decode section 19 of a token 12, processing progresses as follows. First, a verification value is taken out from the verification value attaching part 21 (S41). Hash count is performed about an information identifier and a verification value, and it memorizes to the verification value attaching part 21 by making a count result into a new verification value (S42, S43).

[0100] As shown in drawing 12 , when the verification value output section 22 of a token 12 receives a verification value output request from an information processor 11, processing progresses as follows. First, the verification value memorized by the verification value attaching part 21 is read (S51). After this, the contents of storage of the verification value attaching part 21 are initialized (S52). The electronic signature section 24 is called by making the read verification value into an argument, and a verification value is signed (S53). A signature is attached and outputted after a verification value (S54).

[0101] Explanation of the 1st example is ended above.

[0102] in addition, the law [in / the whole access ticket / count of a exponentiation remainder] published when the user authentication equipment of Japanese Patent Application No. No. 62076 [eight to] and an approach are used combining this invention -- changing n -- law -- n can be used as an information identifier. That is, by the user authentication technique of Japanese Patent Application No. No. 62076 [eight to], decode of certification, for example, code data, is performed for an access ticket (auxiliary information for authentication) using reception, this access ticket, and user-identification information from the exterior. and the law used at this time -- n is used as an information identifier. In that case, after Law n is decoded with the decode equipment inside a token, it will not be taken out, but it will be given from the outside with the information for decode.

[0103] Thus, with constituting, the capacity of the verification value attaching part 21 which must be prepared for the token 12 interior can be pressed down to min, and it becomes possible to make the production cost of a token 12 low.

[0104] [Example which is the 2nd] The 2nd example of this invention is explained below. The example described here adds some functions to the 1st example. It enumerates about the function and effectiveness below.

[0105] ** A function will be recovered, if a token 12 outputs a verification value, suspends a function and receives a message from a pin center,large.

[0106] In order to demand recovery of hysteresis from a user, a token 12 outputs the verification value in the time, and it is made to stop, when outputting a verification value outside, or when it goes through fixed time amount using a clock function (or it

stops autonomously and you may make it require a verification value). In order for a user to recover the function of a token 12, I have a pin center,large transmit and check hysteresis and a verification value, and the message for recovering a function must be received from a pin center,large. The pin center,large should perform electronic signature to the verification value to which the message for functional recovery which a pin center,large publishes was sent by the user.

[0107] ** Also output the verification value in the time of processing the use hysteresis as hysteresis.

[0108] Not only an information identifier but the verification value in the time of generating the hysteresis includes the contents of use hysteresis. It becomes possible to investigate the continuity of each hysteresis later, and it is necessary to be made not to manage hysteresis by the side of an information processor by this strictly (sequence).

[0109] ** Hold an old verification value by the pin center,large side.

[0110] The verification value inside a token was initialized in the old example by the output request from a user. However, the function can be made unnecessary by holding a user's last verification value by the recovery-system side of a pin center,large.

[0111] The configuration of the token 12 in this example is shown in drawing 13 . In addition, the sign which corresponds to the part corresponding to drawing 3 in drawing 13 is attached, and detailed explanation is omitted. this drawing -- setting -- a token 12 -- the user private key attaching part 18, the decode section 19, the verification value generation section 20, the verification value attaching part 21, the token private key attaching part 23, the electronic signature section 24, a control section 30, the hysteresis generation section 31, and counting -- it has the section 32, the pin center,large public key attaching part 33, and the signature verification section 34 grade. In addition, the clock section 35 may be formed if needed.

[0112] It consists of this examples so that the communication link with an information processor 11 may be altogether performed through a control section 30, and a control section 30 processes by calling other processing sections appropriately to the demand from an information processor 11.

[0113] The control section 30 holds the operating state of a token 12 to the interior, and there are the two modes, the normal mode and stop mode, in operating state. In the normal mode, to the decode demand from an information processor 11, a token 12 performs decode processing, as the 1st example described, and it performs processing in which the result is returned. On the other hand, processing of a decode

demand is not received in stop mode. in stop mode, only a functional restart demand (verification value with a pin center,large signature) is received fundamentally, when the demand is just, stop mode is canceled, and processing in which it shifts to the normal mode is carried out (actual -- other than this -- being also alike -- you may make it processing in which the verification value which signed the verification value currently held to the verification value attaching part 21 at the time is outputted also receive).

[0114] The shift to stop mode from the normal mode is based on the count which performed for example, decode processing. counting of drawing 13 -- the section 32 holds the count which performed decode processing. For example, if the count exceeds the counts (for example, 100 etc. times etc.) appointed beforehand, the message of the purport "over which the term passed" will be returned to an information-processor 11 side, and it will shift to stop mode.

[0115] When it has a clock as a configuration, based on the information on the last stopping time held to the control-section 30 interior, it may be made to carry out. That is, when there is a demand from an information processor, a control section compares last time the stopping time and the current time of day which were held in the control section, returns the message of the purport "the term passed" when the time amount (for example, one etc. month etc.) on which it decided beforehand had passed to an information-processor 11 side, and shifts to stop mode.

[0116] Processing of the control section 30 of a token 12 is explained to a detail with reference to drawing 14 - drawing 16 below. In addition, it means that the part shown by the dotted line in drawing 14 - drawing 16 is not processing of a control section 30 but related processing of the configuration section.

[0117] In drawing 14 , either a decode demand, a verification value output request and a functional restart demand are inputted into the control section 30 of a token 12 from an information processor 11. First, it is distinguished for the mode of a control section 30 whether it is stop mode (S61). the time of not being stop mode -- counting -- the enumerated data of the section 32 are read and it is distinguished whether these enumerated data exceeded the reference value, 100 [for example,], (S62, S63). When it is not over 100, it progresses to the node B of drawing 16 , and decode processing etc. is performed. When it is over 100, a verification value with a signature is outputted. That is, read the value of the verification value attaching part 21, the electronic signature section 24 is made to generate a verification value with a signature, and it receives (S64, S65). After this, the message of "shifting to stop mode" with a verification value with a signature is returned to an information

processor 11 (S66). and counting -- the enumerated data of the section 32 are cleared and it shifts to stop mode (S67, S68).

[0118] In step S61, when a control section 30 is stop mode, a decode demand, a verification value output request, and a functional restart demand is distinguished for the received demand (S69, S70, S71). When a demand is a decode demand, the message "it is stop mode now" is returned to an information processor 11, and processing is ended (S72). When a demand is a verification value output request, read the verification value of the verification value attaching part 21, and the electronic signature section 24 is made to generate a verification value with a signature, and it receives (S73, S74). After this, return processing is ended for a verification value with a signature to an information processor 11 (S75). It progresses to the functional re-start process of the node A of drawing 15 at the time of a functional restart demand. When the received demands are not any of a decode demand, a verification value output request, and a functional restart demand, either, an error is returned to an information processor 11 and processing is ended (S76).

[0119] Drawing 15 shows a functional re-start process. In drawing 15 , the received verification value with a pin center,large signature is first passed to the signature verification section 24, and the justification of a signature is verified (S77). If a signature is right, the passed verification value will be compared with the verification value of the verification value attaching part 21, and it will inspect whether both sides are in agreement (S78-S80). If in agreement, the mode of a control section will be made to shift to the normal mode from stop mode, and the message of a "functional restart" will be returned to an information processor 11 (S81, S82). In step S78, when a signature is not right, the message "a signature is not right" is returned to an information processor 11, and processing is ended (S83). When a verification value is not in agreement in step S80, the message "a verification value is not right" is returned to an information processor 11, and processing is ended (S84).

[0120] Drawing 16 shows processing when enumerated data have not exceeded a threshold, 100 [for example,]. In drawing 16 , it is first inspected for a demand whether it is a decode demand (S85). The data which were passed in the decode demand are sent to the decode section 19 (S88). The decode section 19 decodes (S89-S93). Moreover, when a demand is not a decode demand, it is distinguished whether it is a verification value demand (S86). In being a verification value demand, it progresses to the node C of drawing 14 , and verification value output processing is performed. In not being a verification value output request in step S86, either, an error is returned to an information processor 11 and it ends processing (S87).

[0121] Explanation of processing of the control section 30 of a token 12 is finished above.

[0122] In addition, in this example, although it is made to shift to stop mode also when there is a verification value demand from an information-processor 11 side (it shifts to the node C of drawing 14 from step S86 of drawing 16), you may not do so. For example, you may make it return the value which signed the verification value which updates a verification value and is held only at that time to the verification value demand in the normal mode (the last of explanation of this example describes this merit).

[0123] The decode section 19 and the user private key attaching part 18 have the same function as the 1st example.

[0124] The hysteresis generation section 31 generates three groups of the information identifier passed from the decode section 19, and the present verification value, as drawing 16 also showed, and it performs processing in which a control section 30 is passed by making it into use hysteresis.

[0125] The verification value generation section 20 is [0126] to the hysteresis ud passed from the hysteresis generation section 31.

[Equation 3] Hu=Hash(ud)

The becoming hash value is calculated, processing in which it is stored in the verification value attaching part 21 is performed, and the verification value attaching part 21 holds the verification value in the time.

[0127] The electronic signature section 24 performs processing which performs electronic signature to the given value using the private key held like the 1st example at the private key attaching part 23 holding the private key only for the tokens. In this example, further, the signature verification section 34 is formed and processing in which it verifies whether the signature passed using the public key of the pin center,large held at the pin center,large public key attaching part 33 is a signature of a pin center,large is performed. It is possible to use electronic signature techniques, such as a RSA signature, in these configuration sections fundamentally, and since it is a well-known technique, detailed explanation is omitted here.

[0128] The configuration of the information processor 11 in this example is shown in drawing 17 . In drawing 17 , a corresponding sign is given to a corresponding part with drawing 2 . Although it is the almost same configuration as the thing of the 1st example fundamentally, since a token goes into stop mode when it is the information processor 11 of this example, in order to make it resume, I have to transmit hysteresis to a pin center,large, and have to have a restart message to it sent in this drawing.

Then, places with the verification value receive section 36 with a signature which receives a verification value with the signature from a pin center,large differ. Moreover, the configurations of the hysteresis held at the hysteresis attaching part 16 differ.

[0129] The configuration of the recovery system 13 of the pin center,large in this example is shown in drawing 18 . In drawing 18 , a corresponding sign is given to a corresponding part with drawing 5 . In this drawing, when the justification of hysteresis is verified compared with the thing of the 1st example as a configuration, the verification value with a signature of a pin center,large must be sent to an information processor 11, and the configuration section 37 for performing it, i.e., a pin center,large private key attaching part, the electronic signature section 38, and the verification value transmitting section 39 with a signature are extended. Moreover, since the configurations of the use hysteresis sent from an information-processor 11 side differ, the hysteresis naturally processed in the recovery pin center,large also differs.

[0130] The configuration of the use hysteresis held in each part at drawing 19 is shown. (a) is use hysteresis recorded on the hysteresis attaching part 16 of an information processor 11. The contents of each hysteresis have an information identifier as shown in (c), and composition of the pair of the verification value currently held at the token at the time.

[0131] In case hysteresis is sent to a pin center,large from an information processor 11, the verification value to which the signature of a token 12 was attached to the last of the train of the hysteresis is given (b). The verification value with a signature is outputted when a token 12 suspends a function, and a token 12 performs electronic signature to the verification value in the time (d).

[0132] A pin center,large uses the verification value with a signature of (d) for verification of hysteresis. And if it is judged as a result of verification that it is just, the value with which the pin center,large performed electronic signature to the verification value attached at the end as a message for making the function of a token 12 resume will be sent to an information processor 11. It is (e).

[0133] Next, processing of a recovery system 13 is explained. If hysteresis is transmitted from an information processor 11, the hysteresis receive section 25 will receive. The received hysteresis is passed to the signature verification section 29 while it is stored in the hysteresis attaching part 26. The signature verification section 29 chooses the public key of a token 12 connected to the information processor 11 which has transmitted hysteresis from two or more token public keys stored in the token public key attaching part 28, and verifies the signature of hysteresis using the public key. The verification result is held with the hysteresis stored in the hysteresis

attaching part 26.

[0134] After reception of hysteresis finishes, the hysteresis verification section 27 begins to operate. Refer to the verification result of a signature incidental to it for the hysteresis verification section 27 with reference to the hysteresis received now. When the verification result of a signature is not just, processing after this is not performed. If the verification result incidental to hysteresis is just, it will verify whether the contents of hysteresis are still more nearly just.

[0135] Verification processing of the contents of hysteresis is performed as follows.

(1) Suppose that the train of the sent hysteresis is as follows.

(id1,hu0),(id2,hu1),(id3,hu2),...,(idn,hun−1),sign(hun)

However, the verification value in the time of, as for id, the information identifier having been generated and the hysteresis being generated here, as for hu and sign() presuppose that it is the sign of a token.

(2) Discover the verification value at the time of the token having sent last time out of a hysteresis attaching part, and set it to Huold.

(3) Take out the verification value hu0 out of the hysteresis (ID1, hu0) of the beginning of the sent use hysteresis, and confirm whether it is equal to Huold.

(4) Next calculate Hash (id1, hu0), and confirm whether it is set to hu1.

(5) Confirm to the last verification value hun like the following.

(6) If it passes to all inspection, it will be judged that use hysteresis is just.

[0136] Only when hysteresis is judged to be a right thing as a result of verification processing, the last verification value hun is sent to the electronic signature section, and electronic signature is performed with the private key of a pin center,large. And a verification value with the signature of a pin center,large is returned to the information processor which has sent hysteresis.

[0137] In order that a token may suspend a function with constituting as mentioned above at a certain time, the user of the information processor has to send just hysteresis to a pin center,large, in order to make the function of a token resume. Therefore, it becomes possible to demand recovery of hysteresis from a user.

[0138] Moreover, since the last verification value was recorded on the pin center,large side and verification was not only successful even when the part was destroyed for the right hysteresis sent from the token by a certain reason, no maintenance data by the side of a pin center,large change. Therefore, if a token carries out hysteresis with resending in that case, verification will be performed normally.

[0139] moreover -- most parts of others even when verifying hysteresis by the recovery-system side and a part of hysteresis has broken with constituting in this

example so that a token may output a verification value autonomously (lost) -- verification -- possible -- making .

[0140] That is, even when the load of a token is low, hysteresis is verified by the recovery-system side by outputting what signed the verification value which the token holds autonomously at the time not only when a user demands a verification value as having mentioned above, but and a part of hysteresis has broken (lost), about most of other parts, verification becomes possible.

[0141] In this case, the use hysteresis sent to a pin center,large becomes a configuration like drawing 20 . Suppose that hysteresis 25 has been lost in the information-processor side according to a certain accident at this time.

[0142] In the case of use hysteresis which has a verification value as shown previously only in the last, verification of after hysteresis 26 is attained, but in spite of not losing the contents about hysteresis 24 from hysteresis 1, it is unverifiable that it is just.

[0143] When it inserts a verification value with a signature in the middle, and hysteresis 25 is lost in the case of this example, verification only of hysteresis 24 only becomes impossible, and verification of it is attained about the remaining hysteresis. That is, hysteresis 1 to the hysteresis 10 is [hysteresis 23] because each becomes verifiable from hysteresis 37 with the verification value 4 with a signature to hysteresis 57 by the verification value 3 with a signature with the verification value 2 with a signature as for hysteresis 25 to the hysteresis 36 from hysteresis 11 by the verification value 1 with a signature.

[0144] Thus, even when a part of hysteresis is lost by inserting a verification value with a signature into hysteresis at suitable spacing, verification can be made possible about the great portion of remaining hysteresis.

[0145] What is necessary is to form the equipment which judges whether a load is low in the control section inside a token, in order to realize this, and just to generate the verification value with a signature autonomously, when the load of a token is low.

[0146] Moreover, what is necessary is just to constitute so that a verification value with a signature may be outputted by the demand from an information processor, i.e., a user, even if a token does not carry out autonomously. What is necessary is not to branch the node C of drawing 16 to the node C of drawing 14 (step S64) for that purpose, and just to change processing so that a verification value may be updated, a verification value with a signature may be generated and it may be returned to an information processor 11.

[0147] Moreover, the information on time of day can be taken now as use hysteresis

by giving a clock function to a token. By it, a recovery pin center,large side can know now not only the hysteresis which information to only have used but the used time of day. The clock section is the usual clock function, holds a date and time of day, and should just have the function which outputs current time of day according to a demand. What is necessary is just to also combine the information on time of day with the information identifier mentioned above, in order to include time of day in hysteresis. Moreover, if it has a clock function, it will become possible to make it "the time amount which has passed since the time of stopping to last time" as conditions for the shift to the stop mode mentioned above.

[0148] Whenever this prepares the counter section in the interior of a token and outputs hysteresis, in case it counts the value of a counter and outputs hysteresis outside, you may make it output not a verification value but the value of a counter, although it constitutes from this example further again so that the verification value currently held at the time may be given to the hysteresis outputted outside. In that case, the part used as the input of the Hash Function under old explanation serves as a value of the counter currently held at use hysteresis and its time.

[0149]

[Effect of the Invention] As explained above, in order to reduce the amount of data to hold according to this invention, data are not kept in defense equipment, but he outputs out of defense equipment and is trying to keep the small verification value of the amount of data in defense equipment as that substitute. Therefore, the storage capacity and the need throughput of defense equipment can be suppressed. Since a verification value attaches a signature and is sent outside, it can prevent an alteration, and it can ensure verification of data. Moreover, in order to enable restoration of the sequence of data, by adding the information for sequence restoration to data, even if it is data currently kept dispersedly, the sequence can be restored, and verification can be made easy. Furthermore, since it can be made to carry out continuation activation of the related processing when defense equipment receives the value which gave the signature of a just person to the data which defense equipment holds, in order to carry out continuation activation, after winning popularity in a delivery signature, I have to have a just person return the data held in defense equipment. Therefore, the data for verification are inevitably sent to a just person, and the data for verification can be collected certainly. Moreover, if it is made to output a verification value with a signature frequently, even if some data will carry out breakage etc., verification can be ensured about many other data.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the block diagram showing the 1st example of this invention as a whole.

[Drawing 2] It is the block diagram showing the configuration of the information processor 11 of drawing 1 .

[Drawing 3] It is the block diagram showing the configuration of the token 12 of drawing 1 .

[Drawing 4] It is drawing explaining the verification value attaching part 21 of drawing 3 .

[Drawing 5] It is the block diagram showing the configuration of the recovery system 13 of drawing 1 .

[Drawing 6] It is drawing explaining the information decoded in a token 12.

[Drawing 7] It is drawing explaining the configuration of use hysteresis.

[Drawing 8] It is a flow chart explaining processing of the control section 14 of the information processor 11 when there is a use demand of information from a user.

[Drawing 9] It is a flow chart explaining processing of the control section 14 of the information processor 11 when there is a use hysteresis recovery instruction from a user.

[Drawing 10] It is a flow chart explaining processing when the decode section 19 of a token 12 receives a decode demand of the information enciphered from the information processor 11.

[Drawing 11] It is a flow chart explaining processing of the verification value generation section 20 of the token 12 called from the decode section 19 of a token 12.
[Drawing 12] It is a flow chart explaining processing when the verification value output section 22 of a token 12 receives a verification value output request from an information processor 11.
[Drawing 13] It is the block diagram showing the configuration of the token 12 of the 2nd example.
[Drawing 14] It is a flow chart explaining processing of the token 12 of drawing 13 .
[Drawing 15] It is a flow chart explaining processing of the token 12 of drawing 13 .
[Drawing 16] It is a flow chart explaining processing of the token 12 of drawing 13 .
[Drawing 17] It is the block diagram showing functional block realized in the information processor 11 of the 2nd example.
[Drawing 18] It is the block diagram showing the configuration of the recovery system 13 of the 2nd example.
[Drawing 19] It is drawing explaining the configuration of the use hysteresis of the 2nd example.
[Drawing 20] It is drawing explaining other configurations of the use hysteresis of the 2nd example.
[Drawing 21] It is drawing explaining a related technique.
[Description of Notations]
11 Information Processor
12 Token
13 Recovery System
14 Control Section of Information Processor 11
15 Information Attaching Part of Information Processor 11
16 Hysteresis Attaching Part of Information Processor 11
17 Hysteresis Transmitting Section of Information Processor 11
18 User Private Key Attaching Part of Token 12
19 Decode Section of Token 12
20 Verification Value Generation Section of Token 12
21 Verification Value Attaching Part of Token 12
22 Verification Value Output Section of Token 12
23 Token Private Key Attaching Part of Token 12
24 Electronic Signature Section of Token 12
25 Hysteresis Receive Section of Recovery System 13
26 Hysteresis Attaching Part of Recovery System 13

27 Hysteresis Verification Section of Recovery System 13

28 Token Public Key Attaching Part of Recovery System 13

29 Signature Verification Section of Recovery System 13